Sílabo de Gerencia de Seguridad de la Información

I. Datos generales

Código	ASUC 00381			
Carácter	Electivo			
Créditos	3			
Periodo académico	2020			
Prerrequisito	Ninguno			
Horas	**Teóricas:**	2	**Prácticas:**	2

II. Sumilla de la asignatura

La asignatura corresponde al área de estudios de especialidad electiva, es de naturaleza teórico-práctica. Tiene como propósito desarrollar en el estudiante la capacidad de gestionar de manera segura la información en las organizaciones, utilizando estándares nacionales e internacionales de seguridad de la información de acuerdo a la realidad de las organizaciones.

La asignatura contiene: Seguridad de la Información. Normas ISO 27001 y 27002. Gestión de Riesgos ISO 27005, metodologías de riesgo: OCTAVE, MAGERIT, NIST800-30 y Risk IT framework. Planeación de Continuidad de Negocio BCP/DRP (Business Continuity Planning/Disaster Recovery Planning). Atención de Incidentes de Seguridad, NIST800-61. Principios organizacionales básicos como la separación de responsabilidades, mínimo privilegio, accountability, y practicas seguras de gestión de capital humano.

III. Resultado de aprendizaje de la asignatura

Al finalizar la asignatura, el estudiante será capaz de gestionar la seguridad de la información aplicando conceptos, prácticas de gestión de seguridad, implementando un plan de seguridad de la información siguiendo las mejores prácticas de la industria relacionadas con seguridad de la información con el objeto de proteger a la organización de los diferentes riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

IV. Organización de aprendizajes

<table>
<tr><td colspan="3">Unidad I
Gobierno de Seguridad de la Información basado en riesgos</td><td>Duración en horas</td><td>16</td></tr>
<tr><td>Resultado de aprendizaje de la unidad</td><td colspan="4">Al finalizar la unidad, el estudiante será capaz de identificar la estrategia y marco de gobierno de Seguridad de la Información, alineando la estrategia de seguridad a los objetivos de la organización.</td></tr>
<tr><td colspan="2">Conocimientos</td><td>Habilidades</td><td colspan="2">Actitudes</td></tr>
<tr><td colspan="2">✓Estrategia de Seguridad de la información
✓Marco de Gobierno de Seguridad de la información
✓Normatividad de Seguridad
✓Casos de negocio de Seguridad
✓Factores a considerar en la seguridad de la información
✓Métricas de Seguridad</td><td>✓Establece una estrategia de seguridad de la información alineada con las metas y objetivos de la organización e identifica un marco de gobierno (gobernanza) de la seguridad de la información
✓Integra la gobernanza de la seguridad de la información en el gobierno corporativo, estableciendo la normatividad de seguridad de la información, incluyendo políticas, normas, estándares y procedimientos de seguridad de la información.
✓Desarrolla casos de negocios (Business cases) para respaldar las inversiones en seguridad de la información e identifica factores internos y externos de la organización que pueden afectar la estrategia de seguridad de la información.
✓Establece métricas clave de seguridad de la información para medir la efectividad de la estrategia de seguridad de la información.</td><td colspan="2">✓Asume el compromiso de revisar los contenidos previos al dictado de la clase.</td></tr>
<tr><td colspan="2">Instrumento de evaluación</td><td colspan="3">• Rubrica de evaluación</td></tr>
<tr><td colspan="2">Bibliografía (básica y complementaria)</td><td colspan="3">Básica:
• Isaca. (2016). Manual de preparación para el examen CISM. 15° ed. EEUU: ISACA, 2016.
Complementaria:
• Bernard, P. (2012). COBIT® 5 - A Management Guide. 1° ed. Van Haren Publishing.
• Isaca. (2012). COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. EEUU: ISACA.</td></tr>
</table>

	• Isaca. (2012). COBIT 5. Procesos Catalizadores. EEUU: ISACA. • Isaca. (2012). COBIT 5 for Information Security. EEUU: ISACA.
Recursos educativos digitales	• Curso MOOC Cybersecurity: Developing a Program for Your Business Specialization • https://www.coursera.org/specializations/cybersecurity-developing-program-for-business

Unidad II **Gestión y evaluación de riesgos de seguridad de la información**		Duración en horas	16
Resultado de aprendizaje de la unidad	Al finalizar la unidad, el estudiante será capaz de gestionar los riesgos de seguridad de la información a un nivel aceptable en función al apetito de riesgo de las organizaciones, poniendo énfasis en la evaluación de riesgos de seguridad de la información.		
Conocimientos	**Habilidades**	**Actitudes**	
✓ Gestión de riesgos ✓ Evaluación de riesgos ✓ Plan de tratamiento de riesgos ✓ Integración de la gestión de riesgo en los procesos de la Compañía	✓ Define un proceso de gestión de riesgos e identifica los requisitos legales, normativos, organizativos y otros aplicables para gestionar el riesgo de incumplimiento a niveles aceptables. ✓ Identifica los principales marcos de referencia y metodologías de riesgo tales como CobiT5, ISO 31000, ISO 27005, MAGERIT, OCTAVE. ✓ Ejecuta evaluaciones de riesgos de seguridad de la información e identifica, recomienda e implementa opciones de tratamiento / respuesta al riesgo para gestionar el riesgo a niveles aceptables. ✓ Integra la gestión del riesgo de seguridad de la información en los procesos organizaciones y de TI.	✓ Participa activamente en el desarrollo de las actividades grupales en clase.	
Instrumento de evaluación	• Lista de cotejo		

Bibliografía (básica y complementaria)	**Básica:** • Isaca. (2016). Manual de preparación para el examen CISM. 15° ed. EEUU: ISACA. **Complementaria:** • Bernard, P. (2012). COBIT® 5 - A Management Guide. 1° ed. Van Haren Publishing. • Isaca. (2012). COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. EEUU: ISACA. • Isaca. (2012). COBIT 5. Procesos Catalizadores. EEUU: ISACA. • Isaca. (2012). COBIT 5 for Information Security. EEUU: ISACA.
Recursos educativos digitales	• Curso MOOC Identifying, Monitoring, and Analyzing Risk and Incident Response and Recovery • https://www.coursera.org/learn/incident-response-recovery-risks-sscp • Curso MOOC herramientas de análisis y gestión de riesgos • https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html

Unidad III **Desarrollo y Gestión de un Programa de Seguridad**	Duración en horas	16
Resultado de aprendizaje de la unidad	Al finalizar la unidad, el estudiante será capaz de implementar un programa de seguridad de la información alineado a la estrategia de seguridad para el logro de los objetivos organizaciones.	
Conocimientos	**Habilidades**	**Actitudes**
✓Programa de Seguridad de la información ✓Identificación de requisitos de seguridad ✓Recursos de Seguridad de la Información ✓Estándares de Seguridad ✓Programa de sensibilización de usuarios	✓Elabora un programa de seguridad de la información en alineación con la estrategia de seguridad de la información y con los objetivos operativos e identifica y gestiona requisitos para recursos internos y externos para ejecutar el programa de seguridad de la información. ✓Establece procesos y recursos de seguridad de la información para ejecutar el programa de seguridad de la información, y utiliza los principales estándares de seguridad de la información en la organización ✓Formula un programa de sensibilización y capacitación en seguridad de la información para fomentar una cultura de seguridad en la organización e integra los requisitos de seguridad	✓Participa activamente en clases a través de preguntas, comentarios y ejemplos.

✓Integración de requisitos en los procesos	de la información en los procesos de la organización y con terceros.	
Instrumento de evaluación	• Rubrica de evaluación	
Bibliografía (básica y complementaria)	**Básica:** • Isaca. (2016). Manual de preparación para el examen CISM. 15° ed. EEUU: ISACA, 2016. **Complementaria:** • Bernard, P. (2012). COBIT® 5 - A Management Guide. 1° ed. Van Haren Publishing. • Isaca. (2012). COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. EEUU: ISACA. • Isaca. (2012). COBIT 5. Procesos Catalizadores. EEUU: ISACA. • Isaca. (2012). COBIT 5 for Information Security. EEUU: ISACA.	
Recursos educativos digitales	• Articulo: Cómo tener un programa de seguridad de la información actualizado • https://home.kpmg.com/ve/es/home/insights/2016/08/como-tener-un-programa-de-seguridad-de-la-informacion-actualizad.html	

<table>
<tr><td colspan="3">Unidad IV
Gestión de incidentes de Seguridad de la Información</td><td>Duración en horas</td><td>16</td></tr>
<tr><td>Resultado de aprendizaje de la unidad</td><td colspan="4">Al finalizar la unidad, el estudiante será capaz de gestionar los incidentes de seguridad de la información de manera oportuna y dar una respuesta efectiva ante la ocurrencia de los mismos, reduciendo los riesgos relacionados. Asimismo, será capaz de implementar procesos de continuidad de negocio y recuperación de desastres.</td></tr>
<tr><td>Conocimientos</td><td colspan="3">Habilidades</td><td>Actitudes</td></tr>
<tr><td>✓Gestión de incidentes
✓Plan de respuesta a incidentes
✓Identificación de incidentes
✓Investigación de incidentes
✓Notificación de incidentes
✓Plan de continuidad de negocio
✓Plan sustitutoria de desastres</td><td colspan="3">✓Establece y un proceso de gestión de incidentes de seguridad de la información, clasifica y categoriza los incidentes de seguridad de la información.
✓Establece un plan de respuesta a incidentes para garantizar una respuesta efectiva y oportuna a los incidentes de seguridad de la información, y desarrolla e implementa procesos para asegurar la identificación oportuna de incidentes de seguridad de la información que podrían afectar el negocio.
✓Establece y mantiene procesos para investigar y documentar los incidentes de seguridad de la información con el fin de determinar la respuesta y la causa apropiadas mientras se cumplen los requisitos legales, reglamentarios y de organización; estableciendo procesos de notificación y escalamiento de incidentes para garantizar que las partes interesadas apropiadas participen en la gestión de la respuesta a incidentes.
✓Determina las prácticas de gestión de recursos humanos (personal) de TI utilizadas para invocar el plan de continuidad del negocio e identifica el análisis del impacto en el negocio (BIA) relacionado con el plan de continuidad del negocio (BCP).</td><td>✓Muestra actitudes innovadoras ganar – ganar, persistencia positiva, entusiasmo y trabajo en equipo.</td></tr>
</table>

Instrumento de evaluación	• Rubrica de evaluación
Bibliografía (básica y complementaria)	**Básica:** • Isaca. (2016). Manual de preparación para el examen CISM (15° ed.) EEUU: ISACA, 2016. **Complementaria:** • Bernard, P. (2012). COBIT® 5 - A Management Guide. (1° ed.) Van Haren Publishing. • Isaca. (2012). COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. EEUU: ISACA. • Isaca. (2012). COBIT 5. Procesos Catalizadores. EEUU: ISACA. • Isaca. (2012). COBIT 5 for Information Security. EEUU: ISACA.
Recursos educativos digitales	• Curso MOOC Gestión de Incidentes de Seguridad Informática • https://cursosgratuitos.es/mf0488_3-gestion-de-incidentes-de-seguridad-informatica-online/

V. Metodología

El desarrollo de la asignatura será mediante investigación previa de los estudiantes de los conocimientos requeridos, seguido de una exposición teórica complementaria con apoyo audiovisual, y una activa participación de los estudiantes, con tratamiento y exposición de casos en clase, revisión y debate de los controles de lectura asignados y planteamiento de problemas y participación general en la solución de los mismos.

Se publicarán casos de discusión semanales, planteamiento de situaciones de auditoría real y participación general en la definición del informe de riesgos de auditoría.

Se distribuirá material digital de lectura y casos previos a cada clase, haciendo uso de mecanismos virtuales. El material deberá ser estudiado y desarrollado por el estudiante

VI. Evaluación

Modalidad presencial

Rubros	Comprende	Instrumentos	Peso
Evaluación de entrada	Prerrequisitos o conocimientos de la asignatura	Prueba Objetiva	Requisito
Consolidado 1	Unidad I	Rubrica de evaluación	20%
	Unidad II	Lista de cotejo	
Evaluación parcial	Unidad I y II	Prueba de desarrollo	20%
Consolidado 2	Unidad III	Rubrica de evaluación	20%
	Unidad IV	Rubrica de evaluación	
Evaluación final	Todas las unidades	Rubrica de evaluación	40%
Evaluación sustitutoria (*)	Todas las unidades	No aplica	

(*) Reemplaza la nota más baja obtenida en los rubros anteriores

Modalidad semipresencial

Rubros	Comprende	Instrumentos	Peso
Evaluación de entrada	Prerrequisito	Prueba Objetiva	Requisito
Consolidado 1	Unidad I	Rubrica de evaluación	20%
Evaluación parcial	Unidad I y II	Prueba de desarrollo	20%
Consolidado 2	Unidad III	Rubrica de evaluación	20%
Evaluación final	Todas las unidades	Rubrica de evaluación	40%
Evaluación sustitutoria (*)	Todas las unidades	No aplica	

(*) Reemplaza la nota más baja obtenida en los rubros anteriores

Fórmula para obtener el promedio:

PF = C1 (20%) + EP (20%) + C2 (20%) + EF (40%)

Mg. Felipe Néstor Gutarra Meza
Decano
Universidad Continental

Firmado por
FELIPE NESTOR GUTARRA MEZA

CN = FELIPE NESTOR GUTARRA MEZA
O = UNIVERSIDAD CONTINENTAL
T = DECANO
Date: 04/03/2020 20:22